Exploring Security and Privacy Issues in Hospital Information System: An Information Boundary Theory Perspective

Nasriah Zakaria, Jeffrey Stanton, Ph.D., and Kathryn Stam, Ph.D

School of Information Studies, Center for Science and Technology, Syracuse University, Syracuse, New York

Background

A small community hospital (67 beds) in Central New York was undergoing a major technological change within the organization, as they move from the use of several legacy information systems to a hospital-wide information system. The focus of the present research is to explore the privacy and security information issues using a framework called Information Boundary Theory [Stanton, 2002]. IBT explains the motivational factors that lead to the revelation or disclosing of information.

Information Boundary Theory (IBT)

IBT is a synthesis of communication boundary theory (Petronio, 1991), a group-value approach to organizational justice (Alder, 1998) and a general expectancy-valence framework for privacy protection (Stone and Stone, 1990).

Trust motivation: Suggests that the revelation of information can be influenced by the nature of relationship between information transmitter and receiver.

Group-value motivation: Suggests that the revelation of information is regulated because it affects one's status in the valued social group.

Method

As part of the Syracuse Information Systems Evaluation (SISE) Project at Syracuse University's School of Information Studies, we interviewed a group of laboratory workers in the hospital one year prior to a major IS change and returned to interview the the same employees about 1 month after the IS implementation

Result and Discussion

Based on our preliminary investigation of security and privacy issues and their impact on the acceptance of hospital-wide IS implementation, we were able to examine the two factors that influence information boundaries. In a scenario where a trust relationship exists the workers would withhold the confidential information from their client to avoid generating mistrust. For example, a laboratory technician describes his response to a friend who called to ask him to reveal her test results:

> "*Oh yeah, I could have done it. I had access to it. I could do a lot of things if I wanted to. I tell her no. I am very careful about that. I don't want to breach anybody's confidentiality. You know, even though she wanted it, even though it was her information, I still can't.*"

The group-value issue was also used to examine the information boundary when respondents were asked about their reactions to colleagues' security misconduct. Depending on worker's position in the laboratory (IT manager vs. lab technician), their response to this situation is different. The IT manager did not have reservations about disclosing information, while the lab technician would rather withhold some relevant information. In the case of taking action against security misconduct, the differential status and job responsibilities of the two positions inspires different attitudes and behaviors:

IT MANAGER: "I would most definitely (report misconduct) I am in a manager position, I would most definitely confront them about the situation as well as transfer the information that I knew to our laboratory director."

LAB TECHNICIAN: "Depends, I guess. I probably would tell, not the person, but I would mention it to the supervisor, depending on what it is. Not specify person".

To conclude, we are able to understand privacy and security related issues using two interconnected factors (information boundary and motivation) that are proposed by IBT.

		Factor 2: Motivation	
		Trust	Group-valued
Factor 1: Security and Privacy Related Information Boundary	Open	Revealing private/ confidential information when there is strong trust relationship	Revealing security behavior information when you have high status position
	Closing	Withhold private information to avoid breaching confidentiality contract	Withhold security behavior information when you have low status position

References:

1.Alder, G.S. (1998) Ethical issues in electronic performance monitoring a consideration of deontological and teleological perspectives. *Journal of Bussiness Ethics,* 17:729-743

2. Petronio, S.(1991) Communication Boundary Management: a theoretical model of managing disclosure of private information between marital couples. *Communication Theory,* 1:311-335.

3. Stanton, J.M. (2002): Information Technology: a boundary management perspective. In S. Clarke, E. Coakes, G, Hunter and A. Wenn (eds). *Sociotechnical and Human Cognition Elements of Information System.*London: Idea Group, 79-103.

4. Stone, E.F., and D.L Stone (1990) Privacy in organizations: theoretical issues, research findings and protection mechanisms. *Research in Personnel and Human Resource Management,* 8:349-411.